Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Институт математики, физики, информатики и технологии

Кафедра физики, технологии и методики обучения физике и технологии

Система удаленного доступа работников к сети организации на основе OPEN VPN

Выпускная квалификационная работа

Квалификационная работа
допущена к защите
зав.кафедрой
«____»_____2020г
_____
(подпись)

Выполнил:
Нагаев Захар Николаевич
Обучающийся группы ПИВС 1501z
_____
(подпись)

Руководитель:
Алексеевский Петр Иванович
старший преподаватель.
_____
(подпись)

Екатеринбург 2020

РЕФЕРАТ

Нагаев З.Н. РАЗРАБОТКА Удалённого доступа сотрудникам к сети организации через open VPN, выпускная квалификационная работа: —43 стр., рис. 38, библ. 45 назв., приложений 1.

Ключевые слова: VPN, РАЗРАБОТКА Open VPN, Виртуальные сети.

Объект разработки – Удалённый доступ к сети организации через Open VPN

Цель работы – Разработать систему удалённого доступа к сети организации с помощью OpenVPN.

В работе описаны этапы разработки удалённого доступа к сети организации через open VPN. Описаны VPN, протоколы передач и методы шифрования. Проведен анализ VPN, протоколы передач и методы шифрования.

Содержание

Ведение

Виртуальные частные сети (VPN), были созданы из-за потребностей защиты. Оригинальная сеть “ARPANET” имела малую защищенность аутентификаций, а также узлы изначально были доверенными [37]. Простые пользователи осознают недостаточную защищенность своих данных. Учреждения уже давно стали мишенями для хакеров. Годами методы и процедуры медленно усовершенствовались и настраивались для защиты информации. Предприятия хотят защиты как своих данных, так и данных клиентов. Злоумышленники также могут прорваться через национальные брандмауэры. Для защиты своих данных большинство людей могут воспользоваться VPN. Существуют несколько различных технологий VPN, как коммерческих поставщиков, так и проектов с открытым исходным кодом. Одна из самых популярных технологий из программного обеспечения с открытым исходным кодом является “OpenVPN”.

OpenVPN — свободная реализация технологии виртуальной частной сети (VPN) с открытым исходным кодом для создания зашифрованных каналов типа точка-точка или сервер-клиенты между компьютерами. Она позволяет устанавливать соединения между компьютерами, находящимися за NAT и сетевым экраном, без необходимости изменения их настроек. [35]

OpenVPN, может использоваться во многих сферах предприятий и для совершенно различных задач. Но практически всегда конфигурация серверов и клиентов делается с нуля. Наиболее часто используемой моделью развертывания OpenVPN является один сервер с несколькими удаленными клиентами. Сервер устанавливается на предприятия, а клиент устанавливается на персональных компьютерах сотрудников, которые стоят у них дома. Это делается для того что бы сотрудники могли безопасно подключиться к сети предприятия без в вмешательства третьих лиц.

Объект исследования – Система удалённого доступа

Предмет исследования – Удалённый доступ к локальной сети предприятию

Система удаленного доступа к локальной сети представляет собой систему, позволяющую пользователю подключаться к локальной сети через Интернет с помощью другого персонального компьютера. Условием для применения такой опции является включенный компьютер, к которому нужно подключиться, а также установленная и запущенный сервер удаленного доступа.

Цель: Разработать систему удалённого доступа к сети организации с помощью OpenVPN.

Задачи:

- Изучить теоретическую часть по виртуальным сетям, методам шифрования и протоколов передач данных
- Провести анализ виртуальных сетей, методов шифрования и протоколов передач данных
- Установить и настроить сервер openVPN на предприятия
- Разработать простой конфигуратор для клиентов

Глава 1. Теоретические основы и определение основных элементов OpenVPN

1.1 Виртуальные частные сети VPN

VPN создает локальную сеть между несколькими компьютерами в сегментах сети. Машины могут находиться как в одной локальной сети, так и могут быть удалены на большом расстоянии друг от друга через Интернет или они могут даже быть подключены через специальные мультимедиа (беспроводные каналы связи, спутниковая связь, коммутируемая сеть). VPN поставляется с дополнительной защитой, чтобы сделать виртуальную сеть частной. Сетевой трафик проходящий через VPN часто называют внутренним туннелем по сравнению с другими трафиками который находится за пределами туннеля. [40]

На рис 1.1 сетевой трафик показан так, как традиционно проходит через сегменты сети и Интернета. Здесь этот трафик относительно открыт для проверки и анализа, но защищенные протоколы такие как HTTPS и SSH менее уязвимы для злоумышленников.

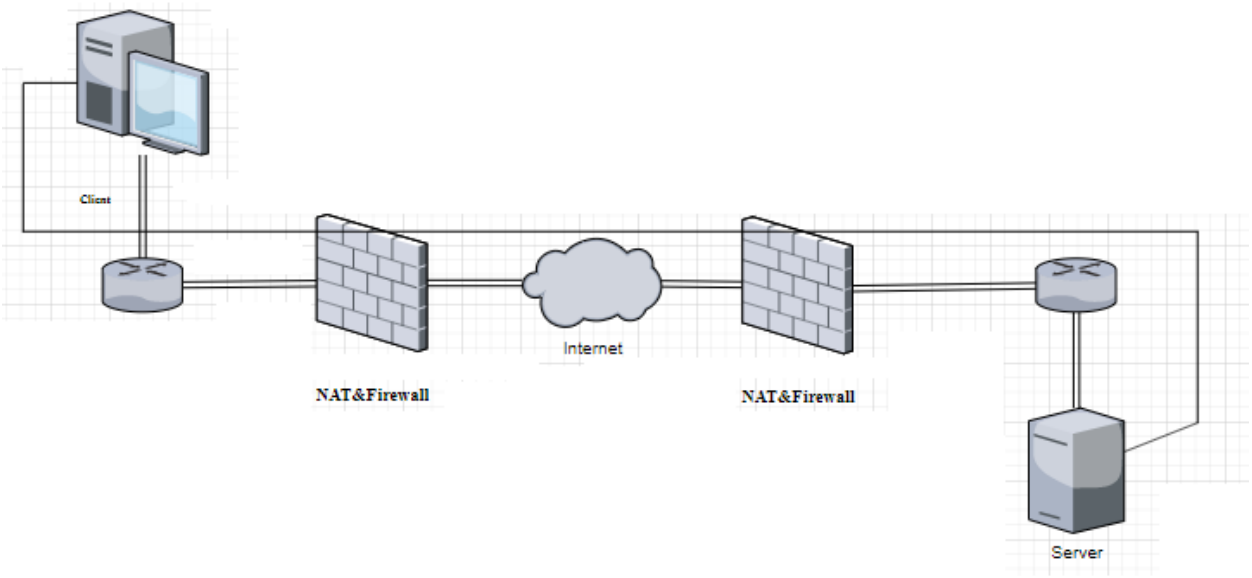

Рис 1.1 сетевой трафик

Здесь злоумышленники по-прежнему могут видеть из какого типа соединения какой компьютер к какому серверу подключён.

Когда используется VPN, трафик внутри туннеля больше не может быть идентифицирован. Трафик внутри VPN может быть любым, что бы не отправлялось по локальной или глобальной сети. В то время как сама VPN маршрутизируется через Интернет, как на рис 1.1, устройства по сетевому пути могут видеть только трафик VPN; эти устройства не знают о том, что происходит или передается внутри частного туннеля. Защищенные протоколы такие как HTTPS и SSH защищены внутри туннеля от других пользователей VPN, но будет дополнительно не опознаваемый трафик снаружи туннеля. VPN не только производит шифрование трафика внутри туннеля, но и также он скрывает и защищает отдельные потоки данных от тех, кто находится за пределами туннеля.

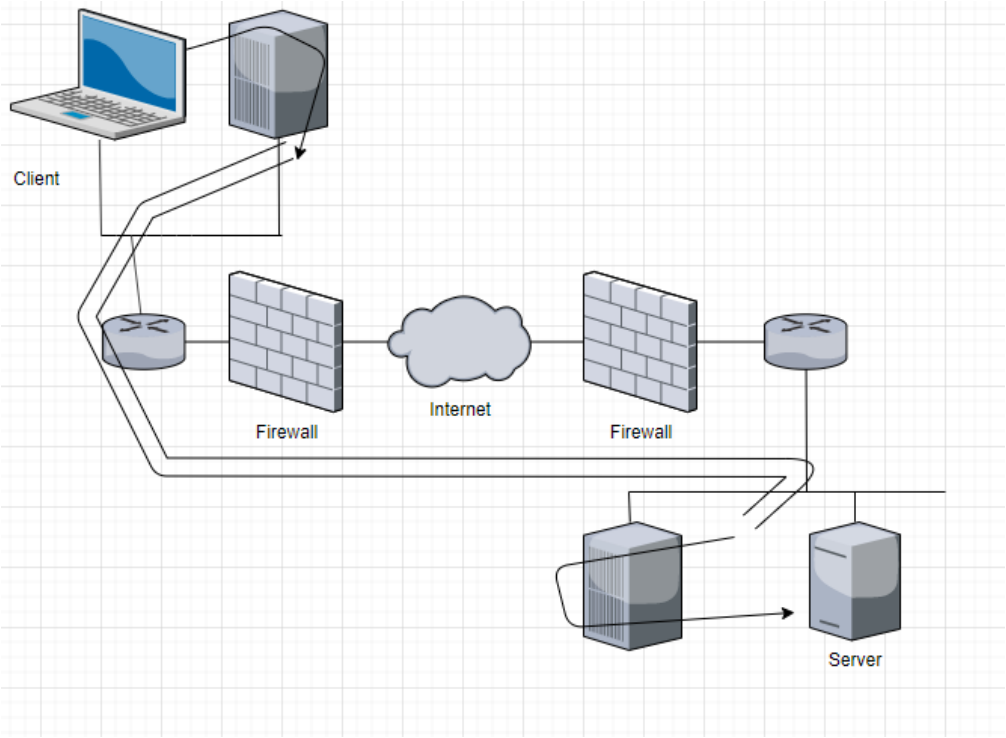

Рис 1.2

На рисунке 1.2 показаны как сильные стороны, так и одна из самая большая угроза технологий VPN. VPN-туннель проникает через роутеры и брандмауэры с обеих сторон. Таким образом весь сетевой трафик, который

проходит через VPN-туннель обходит обычную защиту сети если только не предпринимаются особые меры для контроля VPN трафика. Большинство реализаций VPN используют некоторую форму шифрования и аутентификацию. Шифрование VPN гарантирует что другие стороны, которые отслеживают трафик между системами не может быть декодирован и в дальнейшем не могут быть проанализированы конфиденциальные данные. Аутентификация состоит из двух компонентов:

Первый, аутентификация пользователя и системы, которая предоставляет подключение к авторизованному серверу. Этот тип аутентификации в форме сертификата или сочетании имени пользователя и пароля. Конкретные правила данных пользователей можно согласовать, например, правила о конкретных маршрутах, правила брандмауэра или других скриптов и утилитах. Как правило они уникальны для каждого экземпляра, но для каждого из них можно провести настройку если используется OpenVPN.

Второй компонент аутентификации - это дополнительная защита для

потока связи. В этом случае способ подписи каждого отправленного пакета является установленным. Каждая система проверяет правильно ли подписаны полученные VPN-пакеты до расшифровки данных. Путем аутентификации пакетов, которые уже находятся в зашифрованном виде, система может сэкономить время обработки даже не расшифровывая пакеты, которые не соответствуют правилам аутентификации. Такая аутентификация мешает потенциальным атакам типа “Denial of Service” (DoS), а также предотвращает “Man in the Middle” (MITM) при условии, что ключи подписи хранятся в безопасном месте!

1.2 Типы VPN

Множество продуктов VPN, доступны на рынке как коммерческие, так и с открытым исходным кодом. Все продукты VPN делится на четыре категории:

- VPN на основе PPTP-протокола.
- VPN на основе протокола IPSec.

- VPN на основе SSL.
- OpenVPN.

OpenVPN тоже является VPN на основе SSL поскольку использует SSL или TLS-подобный протокол для установления безопасного соединения. Тем не менее создана отдельная категория для OpenVPN, так как отличается от другой SSL на основе VPN-решение.

1.2.1 PPTP

Одним из протоколов VPN является протокол точка-точка (PPTP) разработан Microsoft и Ascend в 1999 году. Протокол PPTP официально зарегистрирован как RFC263 также PPTP клиент был включен в Windows с 1995 года и до сих пор включен в большинство операционных систем. [33]

В настоящее время протокол PPTP считается небезопасным, так как надежность защищенного соединения напрямую связана с надежностью самого соединения. Пример: аутентификация (пароль). Таким образом ненадежный пароль приводит к небезопасному VPN-соединению. Большинство установок PPTP использует MSCHAPv2 протокол для шифрования паролей. Безопасность протокола PPTP использует сертификаты “X. 509” для защиты PPTP-соединения что приводит к довольно безопасному соединению. Однако не все клиенты PPTP поддерживают EAP-TLS которая необходима для разрешения использования сертификатов “X. 509.”. PPTP использует два канала:

- первый канал управления для настройки соединения
- второй канал для передачи данных.

Канал управления устанавливается через TCP-порт. Канал данных использует общую инкапсуляцию маршрутизации (GRE) протокола, который является IP-протоколом.

PPTP-клиенты доступны практически на всех операционных системах начиная от Windows до Linux и Unix и также для устройств iOS и Android.

1.2.2 IPSec

IPSec является официальным стандартом IEEE/IETF для IP-безопасности. Официально зарегистрирован как RFC2411. IPSec также встроен в стандарт IPv6.[34] IPSec работает на уровне второй и третьей модели OSI сетевой сети. IPSec включает понятие политики безопасности, что делает ее чрезвычайно гибкой и мощной, но также трудно настраиваемой и отлаживаемой. Безопасность политики разрешает администратору шифровать трафик между двумя конечными точками на основе параметров, таких как IP-адрес источника и IP-адрес назначения, а также между исходным и конечным портами TCP или UDP. IPSec можно настроить на использование предварительно разделенных ключей или сертификатов для защиты подключения VPN. Кроме того, он использует сертификаты “X.509”, одноразовые пароли, протоколы имен пользователя или пароль для аутентификации VPN-соединения. Существует два режима работы в IPSec: туннельный режим и транспортный режим.

Транспортный режим используется чаще всего в сочетании с туннелированием второго уровня (L2TP). L2TP протокол выполняет аутентификацию пользователя. Клиенты IPSec встроенные в операционные системы обычно выполняют IPSec с L2TP, также возможно настроить подключение только по протоколу IPSec. IPSec VPN-клиент встроенный в Microsoft Windows по умолчанию используется протокол IPSec с L2TP, но его можно отключить или обойти. IPSec использует два канала:

- Канал управления для настройки соединение и один для передачи данных. Канал управления инициируется через UDP.
- Канал данных использует Инкапсулированную полезную нагрузку безопасности (ESP) протокол который является IP-протоколом.

Целостность IPSec пакетов обеспечивается с помощью проверки подлинности сообщения (HMAC) это тот же метод, который использует OpenVPN. Одним из основных недостатков IPSec является то что многие поставщики

реализовали расширения к стандарту, которые делает его более сложным для того чтобы соединить две конечные точки IPSec от разных поставщиков. Программное обеспечение IPSec входит в состав операционных систем, а также брандмауэры, маршрутизаторы и микропрограммное обеспечение.

1.2.3 VPN на основе SSL

VPN на основе SSL который является на основе протокола SSL и TLS. VPN на основе SSL чаще называют безлимитным VPN или web-VPN, но есть некоторые поставщики, которые предоставляют отдельное клиентское программное обеспечение такое как Cisco AnyConnect и Microsoft SSTP. VPN на основе SSL используют тот же сетевой протокол что и для защищенного веб-сайта (HTTPS), в то время как OpenVPN использует пользовательские форматы для шифрования и подписи данных трафика. Это основная причина, по которой OpenVPN указан как отдельная VPN категория. Не существует четкого определенного стандарта для VPN на основе SSL, но большинство используют Протоколы SSL и TLS для настройки и защитного соединения. В большинстве случаев соединение защищается с помощью сертификатов с одноразовым паролем или протоколами имени пользователя и пароля для аутентификации соединения. На основе SSL, VPN очень похожи на соединения, используемые для защиты веб-сайтов (HTTPS) также часто используется один и тот же протокол и канал (TCP и порт 443). Несмотря на то, что VPN на основе SSL часто называют веб или клиентскими, там есть довольно много поставщиков которые используют плагин браузера или элемент управления ActiveX чтобы улучшить VPN-соединение. Это делает VPN несовместимыми с неподдерживаемыми браузерами или операционными системами.

1.2.4 OpenVPN

OpenVPN это VPN на основе SSL так как он использует протоколы SSL и TLS для защищённого соединение. Однако OpenVPN также использует

HMAC в сочетании алгоритма хеширования для обеспечения целостности пакетов. OpenVPN может быть настроен для использования предварительно разделенных ключей, а также сертификатов. Эти функции обычно не доступны другими VPN на основе SSL. Кроме того, OpenVPN использует виртуальный сетевой адаптер устройство tun или tap в качестве интерфейса между пользовательским программным обеспечением OpenVPN и операционными системами. Как правило любая операционная система поддерживающая устройство tun или tap может работать в OpenVPN. В настоящее время это включает Linux, Free / Open / NetBSD, Solaris, AIX, Windows и Mac OS, а также устройства iOS и Android. Для всех этих платформ клиентское программное обеспечение должно быть установлено что отличает OpenVPN от client-less или веб-VPN. Протокол OpenVPN не определен в стандарте RFC, но протокол является общедоступным, потому что OpenVPN-это часть программного обеспечения с открытым исходным кодом. Факт, того что он является открытым исходным кодом, практически делает OpenVPN более безопасным чем closedsource VPN так как код постоянно проверяется разными людьми. Также существует очень мало шансов что секретные бэкдоры будут встроены в OpenVPN. OpenVPN имеет определение канала управления и канала передачи данных оба из которых шифруются и защищаются по-разному. Однако весь трафик проходит через одно соединения UDP или TCP. Канал управления шифруется и защищается с помощью SSL и TLS каналов, также данные шифруется с помощью пользовательского протокола шифрования. Протокол и порт по умолчанию для OpenVPN это UDP и порт 1194.

1.3 Анализ VPN сетей

1.3.1 Преиущества и недостатки PPTP

Преимуществом VPN на основе PPTP является то, что клиентское программное обеспечение VPN встроено в большинство операционных

систем. Кроме того, время запуска для настройки и инициализация PPTP VPN-соединения происходит очень быстро.

Недостатками VPN на основе PPTP являются отсутствие безопасности и параметры конфигурации как на стороне клиента, так и на стороне сервера. Кроме того, EAP-TLS расширение которое позволяет использовать сертификаты “X.509”, полностью поддерживается только в Microsoft Windows, но существует patch для pppd с открытым исходным кодом. Patch pppd включен в почти каждый дистрибутив Linux. Кроме того, если необходимо прибегнуть к использованию EAP-TLS, то простота настройки PPTP VPN значительно снижается. Это потому, что EAP-TLS требуется настроить инфраструктуру открытых ключей, как IPSec и OpenVPN. Еще одним серьезным недостатком PPTP является использование протокола GRE, который делает его несовместимым с устройствами за пределами NAT.

1.3.2 Преимущества и недостатки IPSec

Преимущества протокола IPSec - это его безопасность, хорошая поддержка со стороны различных поставщиков и платформ включая маршрутизаторы xDSL и Wi-Fi, а также возможность использования Fine-Grained политик безопасности для управления потоком трафика. Недостатками IPSec является то, что его, как известно трудно настроить и отладить. Различные реализации IPSec от поставщиков не воспроизводятся хорошо в месте, и IPSec не интегрируется хорошо с сетями NAT. Наиболее примечательно что не рекомендуется, а иногда даже невозможно запускать сервер IPSec, который находится внутри Сети NAT.

1.3.3 Преимущества и недостатки VPN на основе SSL

VPN на основе SSL или веб-VPN имеют преимущество в отсутствии или очень малого клиентского программного обеспечения. Это делает установку и инициализацию на стороне клиента очень простой. Недостатком веб-VPN можно назвать то, что он часто не является полноценным VPN и позволяет

получить доступ к одному серверу или набору серверов. Кроме того, это усложняет возможность поделиться локальными данными с удаленного сайта или сервера.

1.3.4 Преимущества и недостатки OpenVPN

Преимуществами OpenVPN является простота установки конфигурации и возможность установки в ограниченных сетях, включая сети NAT. Кроме того OpenVPN включает в себя функции безопасности, которые так же сильны, как и у VPN на основе IPSec, включая аппаратную маркерную защиту и поддержку для различных пользователей механизм аутентификации.

Недостатки OpenVPN находятся в его отсутствии масштабируемости и ее зависимость в установке клиентского программного обеспечения. Еще одним недостатком является отсутствие Графического интерфейса для настройки и управления. В частности, драйвер интерфейса tap для Microsoft Windows часто вызывала проблемы развертывания, когда выпускалась новая версия Windows.

1.4 Внутренние компоненты OpenVPN

1.4.1 Драйвера tun и tap

Одним из основных блоков OpenVPN является драйвер tun и tap. Концепция драйвера tun и tap происходит из Unix и Linux, где они часто доступны как часть операционной системы. Это виртуальные сетевые адаптеры, которые рассматривается операционной системой как двухточечный адаптер (в стиле tun) для трафика IP или в качестве полноценного виртуального адаптера Ethernet для всех типов трафиков (в стиле tap). На внутренней стороне этих адаптеров находится приложение такое как OpenVPN для обрабатывания входящий и исходящий трафиков. Linux, Free / Open / NetBSD, Solaris и Mac OS включают в себя драйвер ядра tun. Недавно аналогичный драйвер был добавлен в AIX, который производная от Unix от IBM.

Для Microsoft Windows был написан James Yonan специальный драйвер NDIS, называется адаптером TAP-WIN32[42]. На данный момент версии NDIS5 и NDIS6 драйвера доступны, поддерживая Windows XP через Windows 8.1. Разработка этого адаптера теперь официально отделена от основного OpenVPN развития, но OpenVPN продолжает сильно полагаться на него.

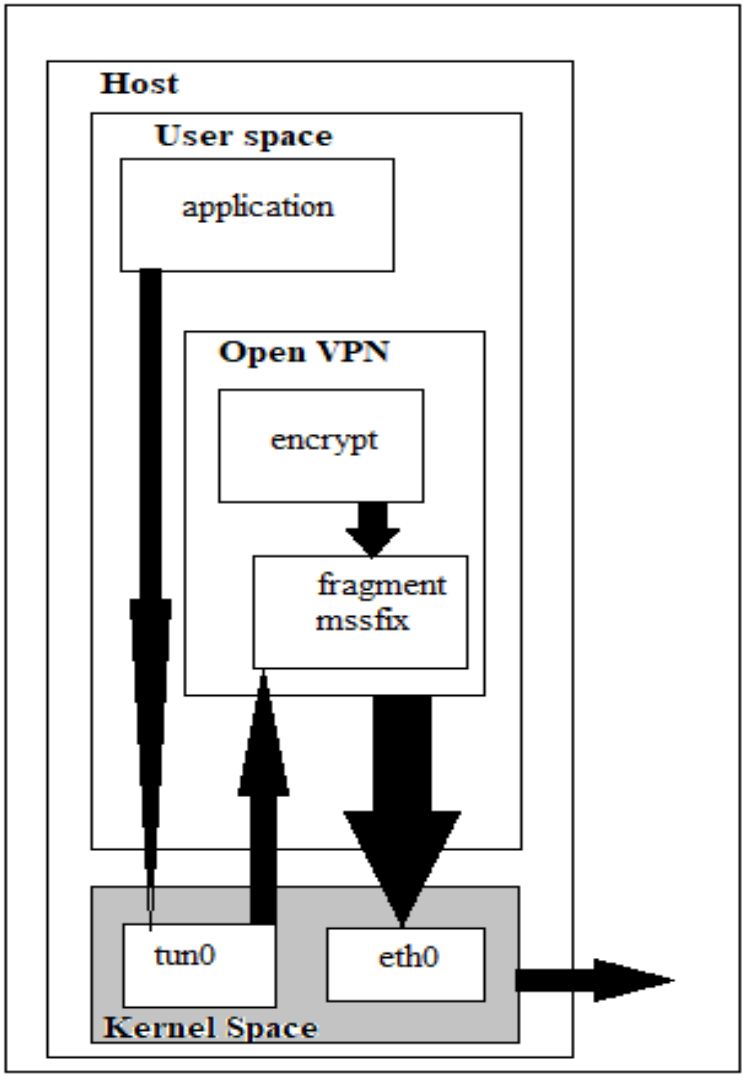

Рис 1.3 Поток трафика из пользовательского приложения через OpenVPN

Пример: Поток трафика из пользовательского приложения через OpenVPN изображен на Рис 1.3. приложение отправляет трафик на адрес, доступный через туннель OpenVPN в несколько шагов:

1. Приложение передает пакет операционной системе.

2. ОС решает использовать обычные правила маршрутизации (пакет должен маршрутизироваться через VPN).

3. Пакет пересылается на устройство настройки ядра.

4. Устройство настройки ядра пересылает пакет в процесс OpenVPN (в пользовательском пространстве).

5. Процесс OpenVPN шифрует и подписывает пакет и фрагментирует его при необходимости, а также снова передает его к ядру (чтобы отправить его на адрес удаленной конечной точки VPN).

6. Ядро забирает зашифрованный пакет и пересылает его на удаленную конечную точку VPN, где происходит обратный процесс.

На этой диаграмме также видно, что производительность OpenVPN всегда будет ниже, чем у обычного сетевого подключения. Для большинства приложений, потеря производительности минимальна и доступна. Однако для скоростей, превышающих 1 Гбит/с, существует слабое место в производительности как с точки зрения пропускной способности так и с задержки. Следует отметить что производительность драйвера Windows намного ниже чем производительность встроенных адаптеров tun и tap в других операционных системах. Это верно даже для самой реализации драйвера TAP-Win32 в NDIS6. Для одного клиента OpenVPN воздействие довольно мало. Для крупномасштабного сервера OpenVPN, который обслуживает много клиентов, это может легко вызвать проблемы с производительностью. Это одна из главных причин того, что сообщество разработчиков открытого исходного кода обычно рекомендует использовать хост на основе Unix или Linux в качестве сервера OpenVPN.

1.5 Режимы UDP и TCP

OpenVPN поддерживает два способа связи между конечными точками, используя UDP или TCP. UDP - это протокол без установленного соединения или с потерями протокола. Если пакет теряется при передаче, то сетевое

соединения незаметно исправит. TCP - это протокол ориентированный на соединение. Пакеты отправляются и доставляются по протоколу handshake, обеспечивая доставку каждого пакета на другую сторону. Оба способа связи имеют свои преимущества и недостатки. Это на самом деле зависит от типа трафика, который отправляется через VPN-туннель.

Пример: Использование приложения на основе TCP через VPN может привести к двойной потере производительности особенно если имеется плохое подключение к сети. В этом случае повторяется передача потерянных пакетов, потерянных как внутри, так и снаружи туннеля, что приводит к снижению производительности. Однако аналогичным образом можно утверждать, что отправка пакетов через UDP, также не является отличной идеей. Если приложения, использующие UDP протокол для своего трафика восприимчивого к атакам удаления или переупорядочения, а базовое зашифрованное TCP соединение повысит безопасность таких приложений даже больше чем базовый VPN на основе UDP. Если большая часть трафика через VPN основана на UDP, тогда лучше использовать TCP-соединение между конечными точками VPN. При выборе между транспортом UDP или TCP, общее правило таково: если у вас работает UDP (mode udp), то используйте его; если нет, то попробуйте TCP (режим tcp-сервера и режим tcp-клиента). Некоторые коммутаторы и маршрутизаторы неправильно пересылают трафик UDP, что может быть проблемой, особенно если несколько клиентов OpenVPN подключены к одному коммутатору или маршрутизатору. Точно так же на производительность OpenVPN через TCP может сильно повлиять выбор Интернет-провайдеров (ISP), некоторые провайдеры используют странные размеры MTU или пакеты, с фрагментированными правилами, что приводит к крайне низкой производительности OpenVPN-overTCP по сравнению с незашифрованным TCP-трафиком.

1.6 Протокол шифрования

OpenVPN реализует TLS через UDP, но способ OpenVPN использования TLS отличается от способа веб-браузера, использующего TLS. Таким образом, когда OpenVPN запускается через TCP, то трафик отличается от обычного трафика TLS. Брандмауэр, использующий глубокую проверку пакетов (DPI), может легко отфильтровать трафик OpenVPN. Основное различие между OpenVPN-TLS и browser-TLS заключается в подписи пакетов. OpenVPN предлагает функции для защиты от DoS-атак с помощью подписания пакетов канала управления с помощью специального статического ключа (--tls-authta.key 0|1). Пакеты канала передачи данных, которые передаются по тому же UDP или TCP соединению, подписываются совершенно по-разному и очень легко различаются от трафика HTTPS. Это также является основной причиной, почему port-sharing, где OpenVPN и безопасный веб-сервер могут использовать один и тот же IP-адрес, и номер порта может фактически работать.

1.7 Режим клиент - сервер с tun и tan Устройствами

Модель развертывания OpenVPN-это один сервер с несколькими удаленными клиентами, способными маршрутизировать трафик.

Основное различие между режимом tun и tap - это тип используемого адаптера. Tap адаптер обеспечивает полный виртуальный интерфейс Ethernet (Второго уровня), в то время как адаптер tun рассматривается как адаптер точка-точка (Третьего уровня) большинством операционных систем. Компьютеры, подключенные с помощью (виртуальных) адаптеров Ethernet, могут образовывать единый широковещательный домен, который необходим для определенных приложений. С точка-точка адаптерами этого невозможно. Кроме того, не все операционные системы поддерживают tap адаптеры. Например: iOS и Android поддерживают только устройства tun. Кроме того, режим tap позволяет настроить мост, где обычная сеть адаптера соединена мостом с виртуальным адаптером tap.

Глава 2. Разработка OpenVPN для организации

2.1 Устоновка и настройка Сервера OpenVPN

Для создания ключей и сертификатов Сервера необходимо сделать:

Открыть папку “easy-rsa”, которая находится по адресу “C:\OpenVPN\easy-rsa” Найти файл vars.bat.sample. Рис 2.1

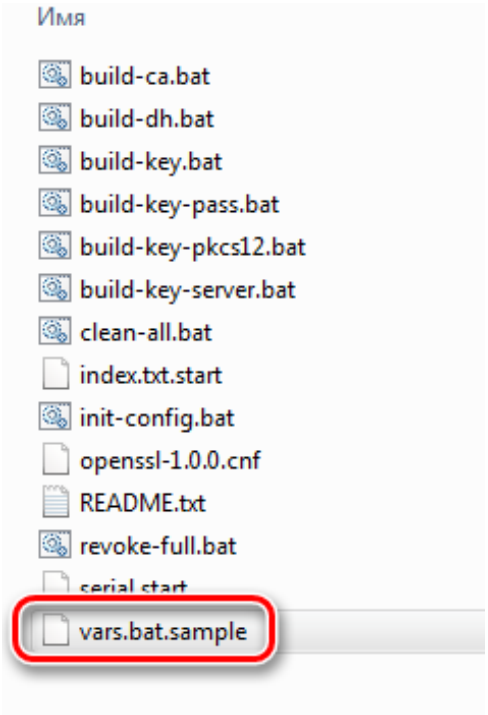

Рис 2.1

Переименовать его в “vars.bat” и открыть его любым текстовым редактором. Рис 2.2

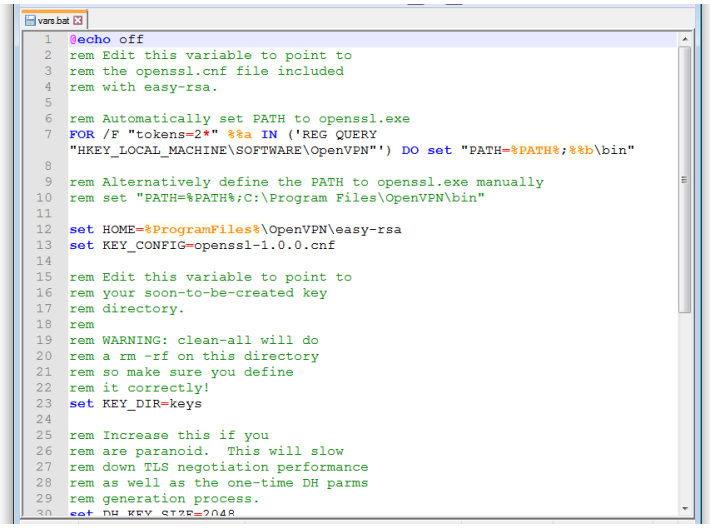

рис 2.2

Удалить все комментарии, выделенные зеленым цветом. рис 2.3

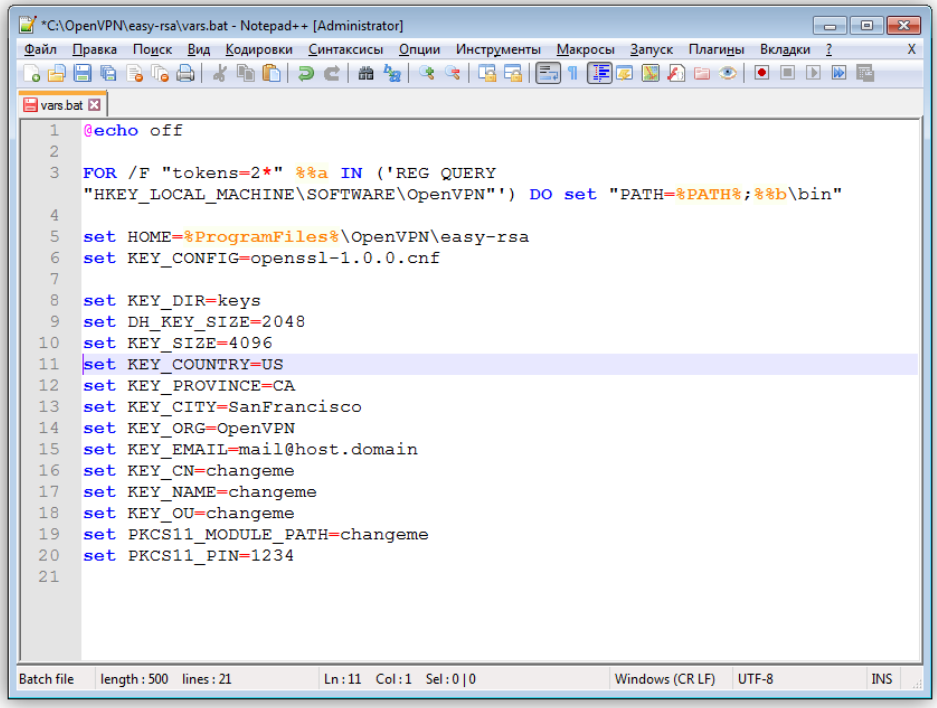

Рис 2.3

Указать путь к папке “easy-rsa” на “C:\OpenVPN\easy-rsa” рис 2.4

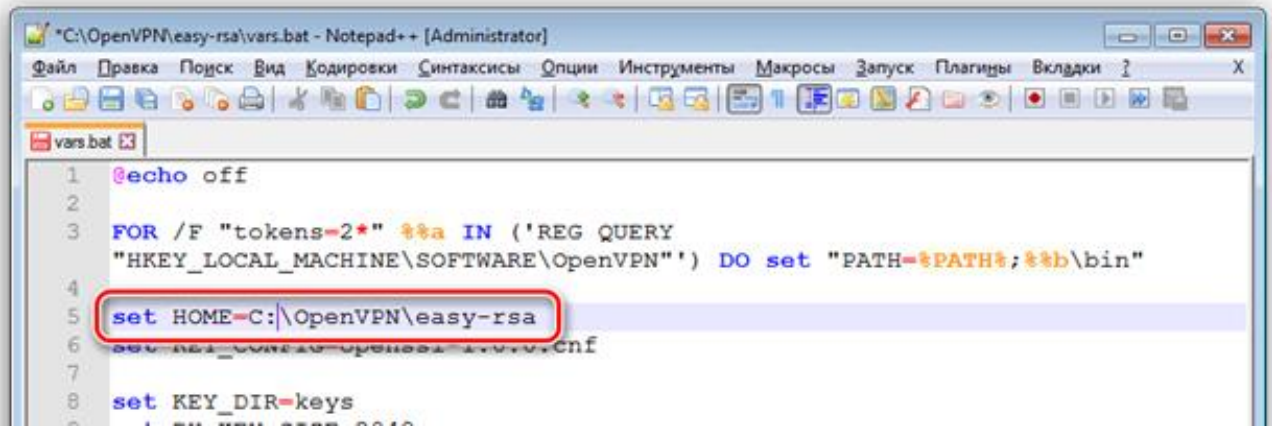

Рис 2.4

Следующие четыре параметра оставить без изменений. Рис 2.5

set key dir = “папка где будут создастся ключи”

set DH key size =” Размер ключа DH”

set KEY_SIZE=” Размер ключа”

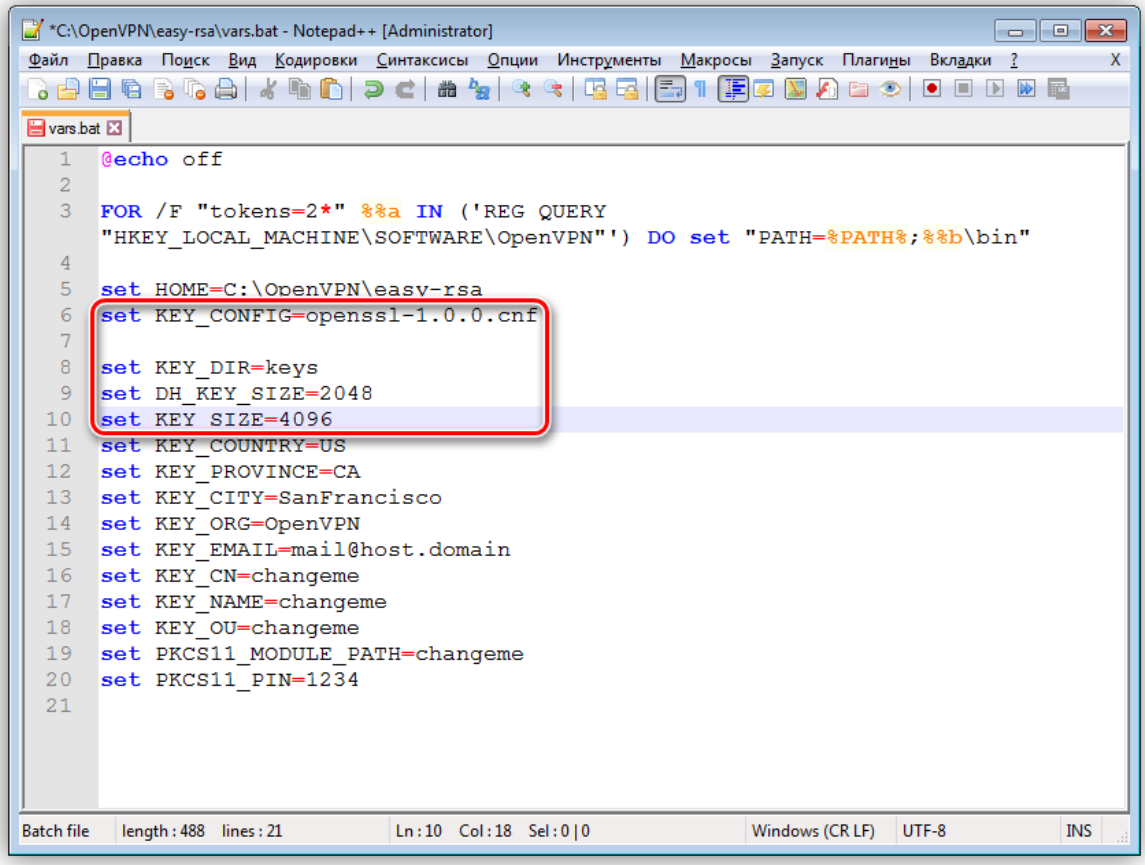

Рис 2.5.

Остальные строки заполнить произвольно. Рис 2.6.

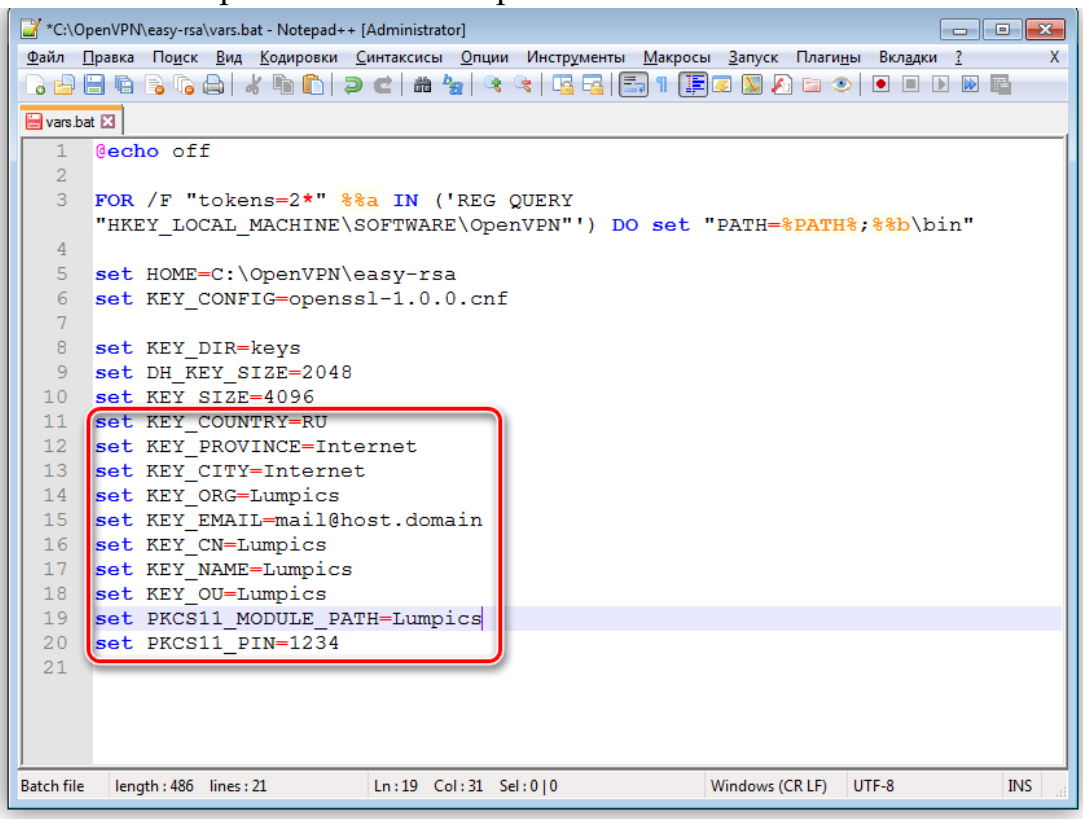

Рис 2.6

Отредактировать следующие файлы: build-ca.bat, build-dh.bat, build-key.bat, build-key-pass.bat, build-key-pkcs12.bat и build-key-server.bat рис 2.7

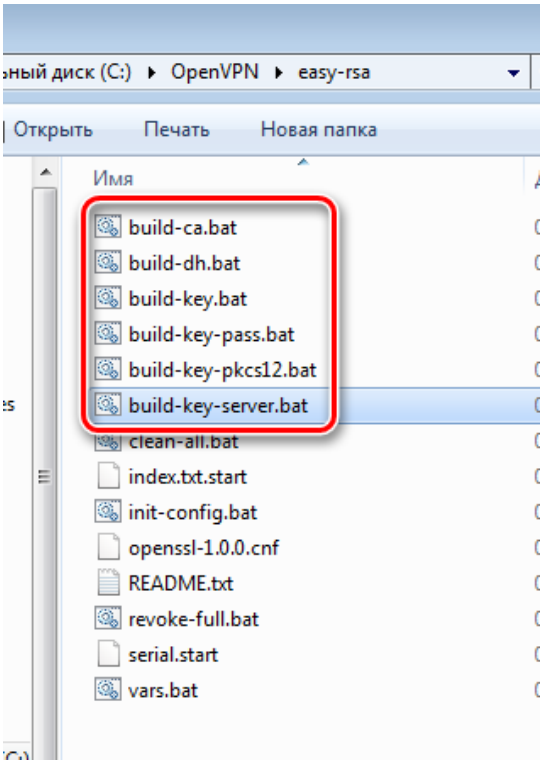

рис 2.7

В них отредактировать команду openssl на полный путь к соответствующему ей файлу “openssl.exe.” рис 2.8

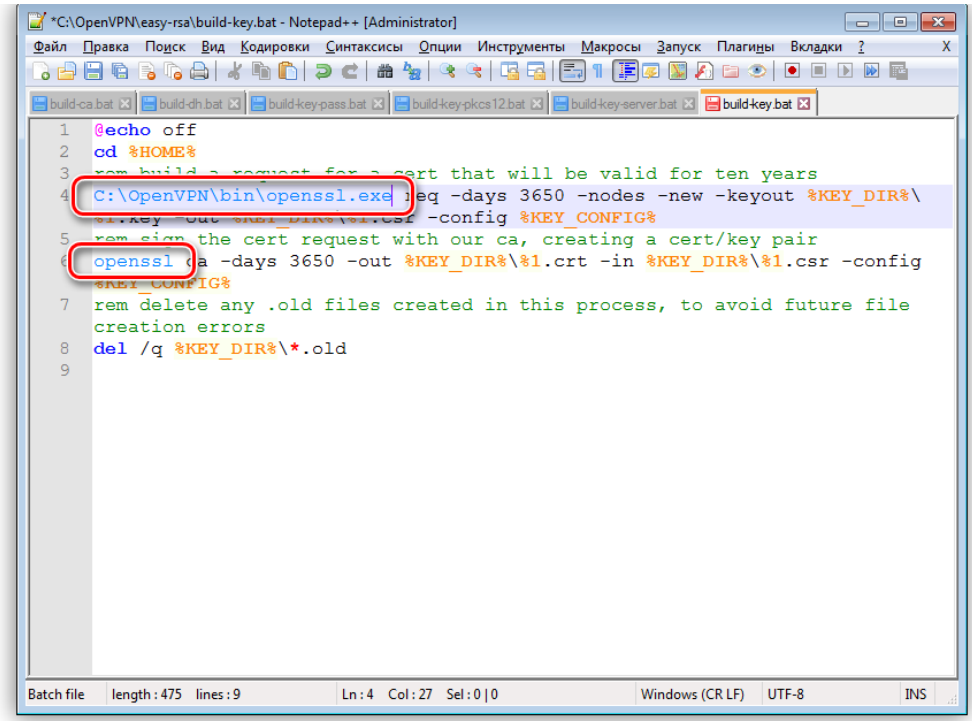

рис 2.8

Открыть папку “easy-rsa”, зажать SHIFT и кликаю ПКМ по свободному месту (не по файлу). В контекстном меню выбирать пункт “Открыть окно команд”. Рис 2.9

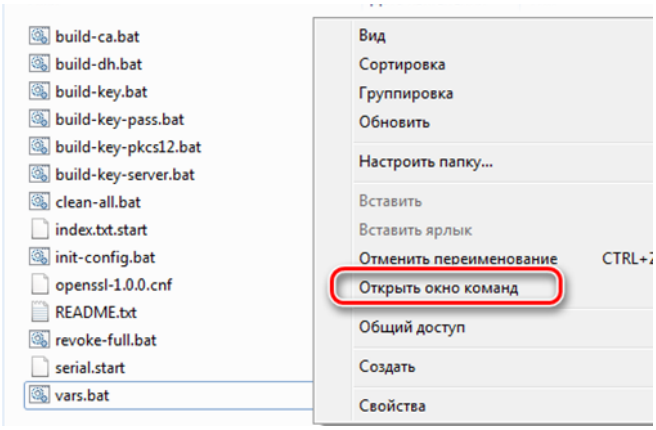

Рис 2.9

Запустится “Командная строка” с уже осуществленным переходом в целевой каталог. Рис 2.10

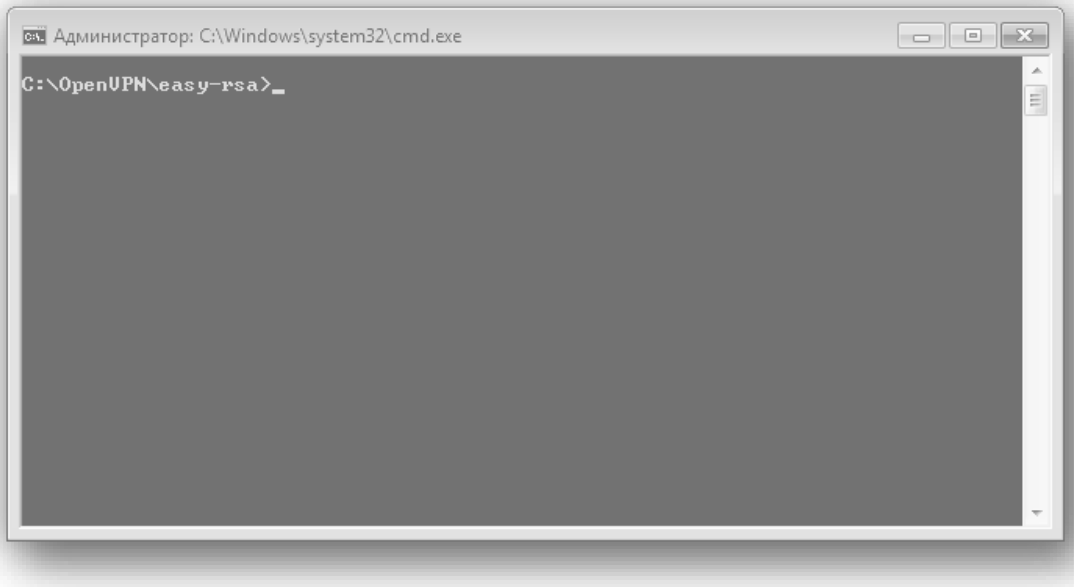

рис 2.10

Вести команду “vars.bat” и нажать ENTER. Рис 2.11

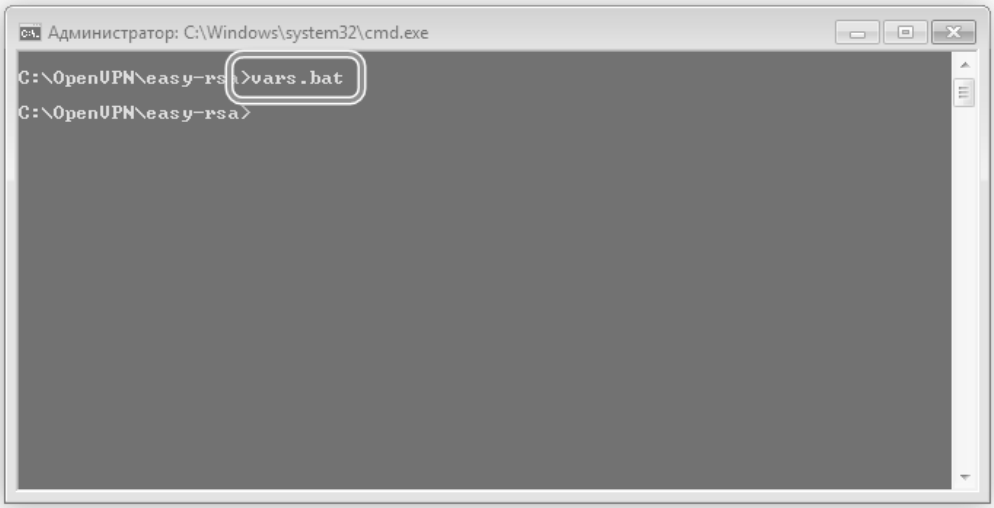

Рис 2.11

Вести команду clean-all.bat рис 2.12

рис 2.12

Повторить, первую команду “vars.bat”. рис 2.13

рис 2.13

Создаем необходимые файлы. Для этого использую команду “build-ca.bat”. После выполнения система предложит подтвердить данные, которые вносились в файл vars.bat. Несколько раз нажать ENTER, пока не появится исходная строка. рис 2.14

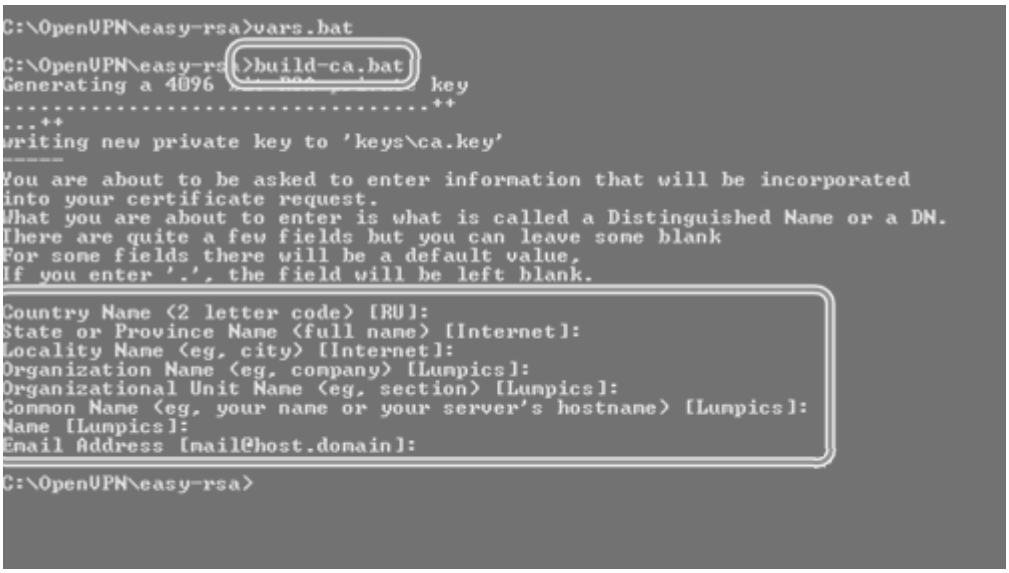

рис 2.14

Создать DH-ключ с помощью запуска файла через команду “build-dh.bat” рис 2.15

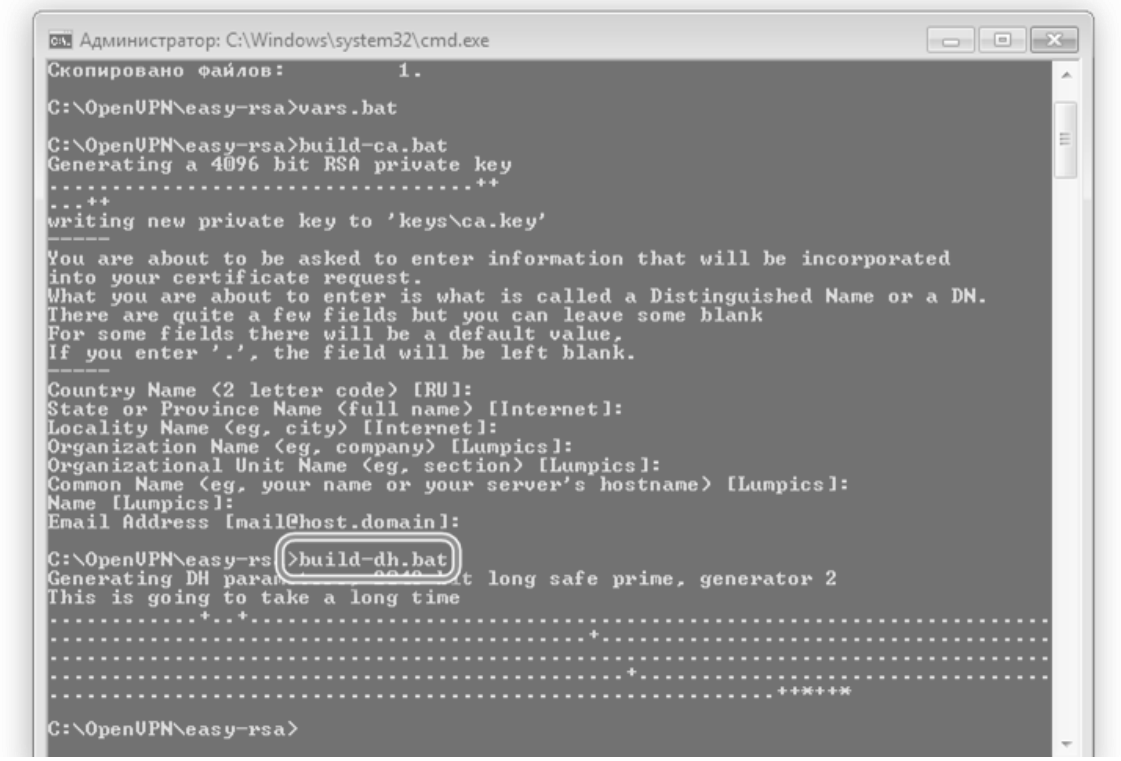

рис 2.15

Приготовить сертификат для серверной части. Ему присвоить то имя, которое прописал в vars.bat в строке “KEY_NAME” это Lumpics. Команда выглядит следующим образом: build-key-server.bat Lumpics. Подтвердить данные с помощью клавиши ENTER, а также два раза согласится, водя букву “y”(yes) Рис 2.16. Командную строку закрыть.

Рис 2.16

В папке “easy-rsa” появится новая папка с названием “keys”. Рис 2.17

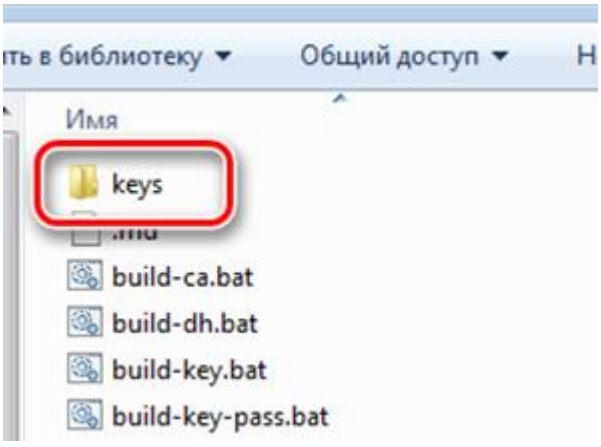

рис 2.17

Содержимое папки “keys”. скопировать в папку “ssl”, которую нужно создать в корневом каталоге программы. Рис 2.18

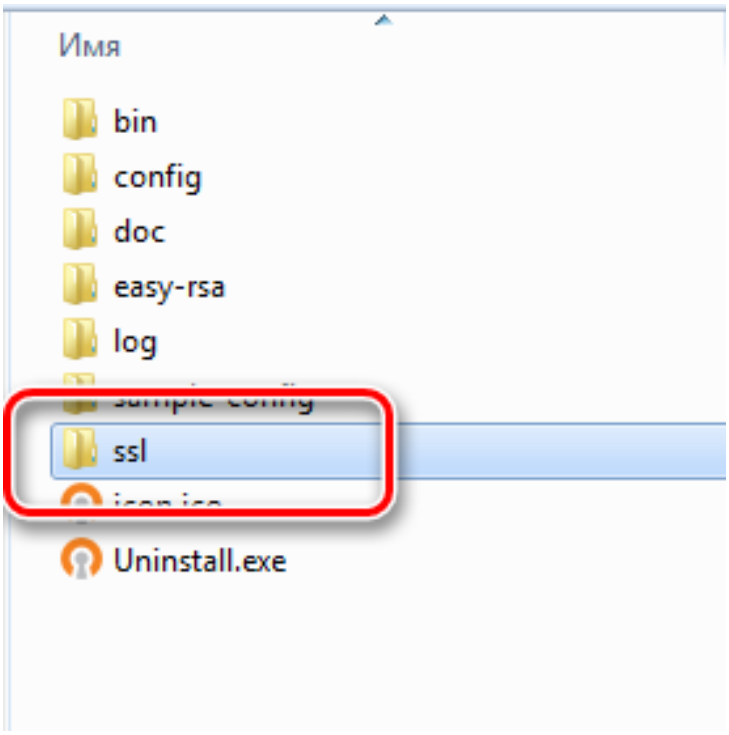

Рис 2.18

Вид папки после вставки скопированных файлов рис2.19

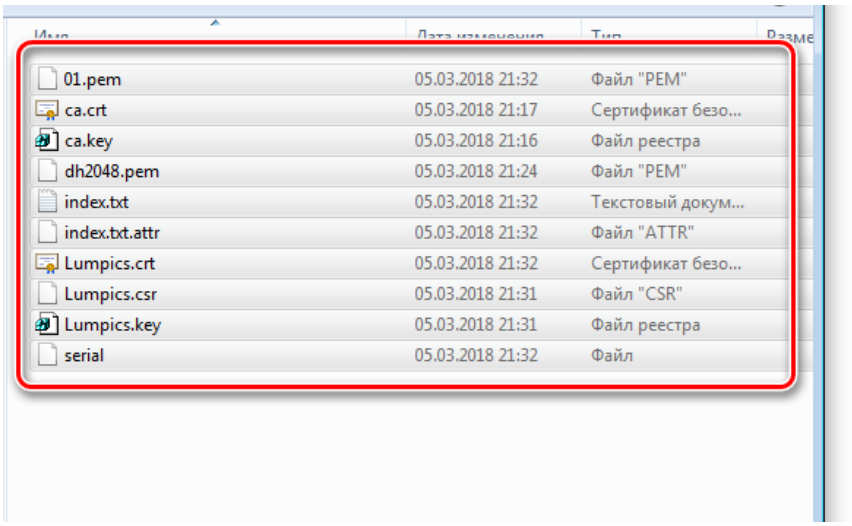

рис 2.19

Открыть каталог “C:\OpenVPN\config”. Создать текстовый документ, переименовать его в “server.ovpn” и открыть. Вести следующий код:

port 443 - порт через который будет подключения

proto udp протокол через который будет подключения

dev tun – виртуальный сетевой драйвер

dev-node "VPN Lumpics" - устанавливает имя виртуального интерфейса

dh C:\\OpenVPN\\ssl\\dh2048.pem – путь к DH ключу

ca C:\\OpenVPN\\ssl\\ca.crt - путь к сертификату

cert C:\\OpenVPN\\ssl\\Lumpics.crt - путь к сертификату

key C:\\OpenVPN\\ssl\\Lumpics.key - путь к ключу

server 172.16.10.0 255.255.255.0 - ip сервера

max-clients 32 – максимальное количество клиентов

keepalive 10 120 - команда является совмещением сразу двух команд ping и ping-restart. Использует сразу два параметра в секундах, перечисленных через пробел

client-to-client - команда предназначена для того чтобы клиенты видели друг друга в сети.

comp-lzo - параметр сжатия трафика, идущего через виртуальный туннель

persist-key указывает не перечитывать файлы ключей при перезапуске туннеля.

persist-tun данная опция оставляет без изменения устройства tun/tap при перезапуске OpenVPN.

cipher AES-256-CBC - алгоритм шифрования

status C:\\OpenVPN\\log\\status.log - указывает путь к статус-файлу, в котором содержится информация о текущих соединениях и информация о интерфейсах TUN/TAP

log C:\\OpenVPN\\log\\openvpn.log - указываем лог-файл

verb 4 - устанавливает уровень информативности отладочных сообщений

mute 20 – количество сообщений логов из одной категории

Для Работы виртуального адаптера нужно:

Открыть Панель управления -Центр управления сетями. Рис 2.20

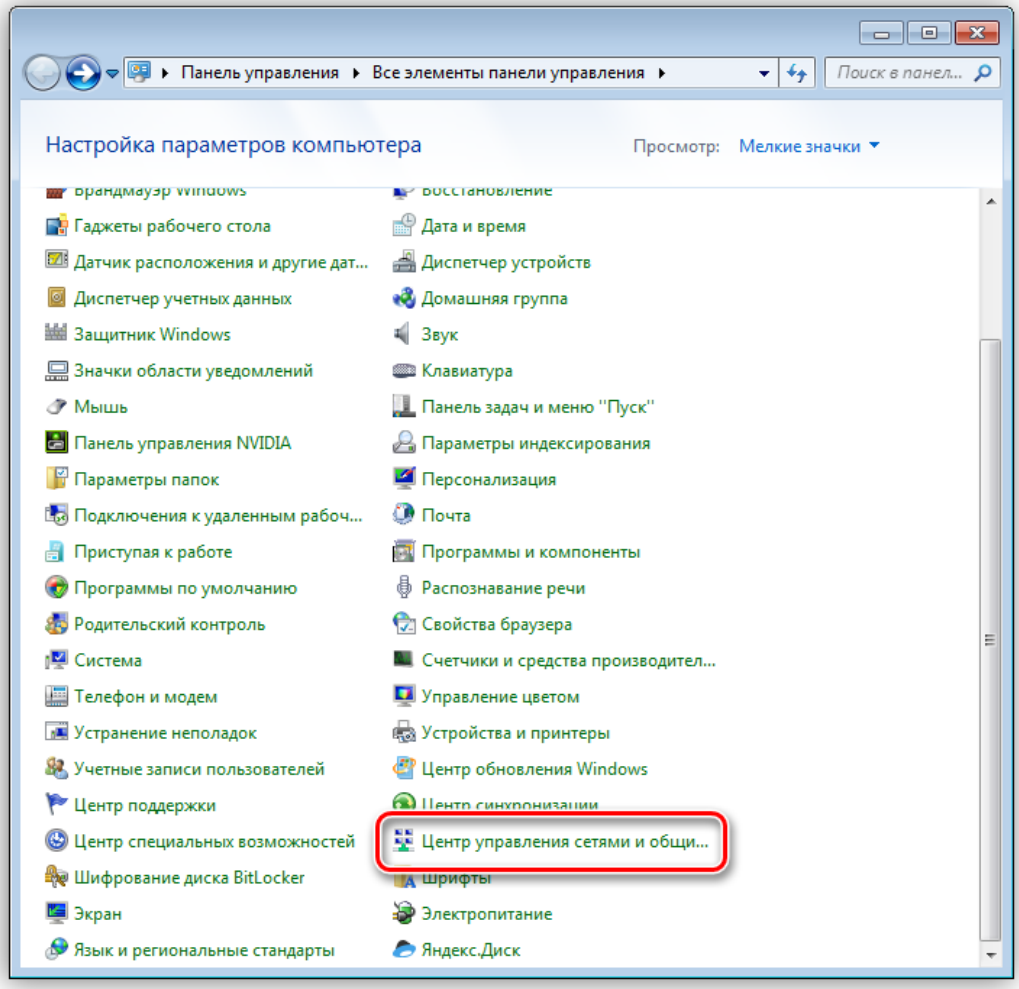

Рис 2.20

Нажать на ссылку слева “Изменение параметров адаптера”. Рис 2.21

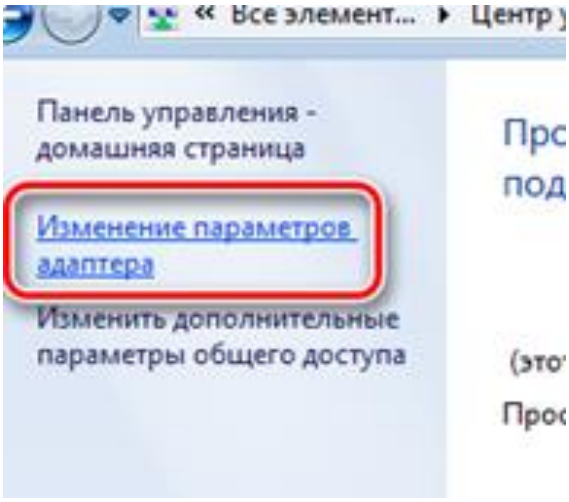

Рис 2.21

Найти подключение, осуществляемое через “TAP-Windows Adapter V9”. Рис 2.22

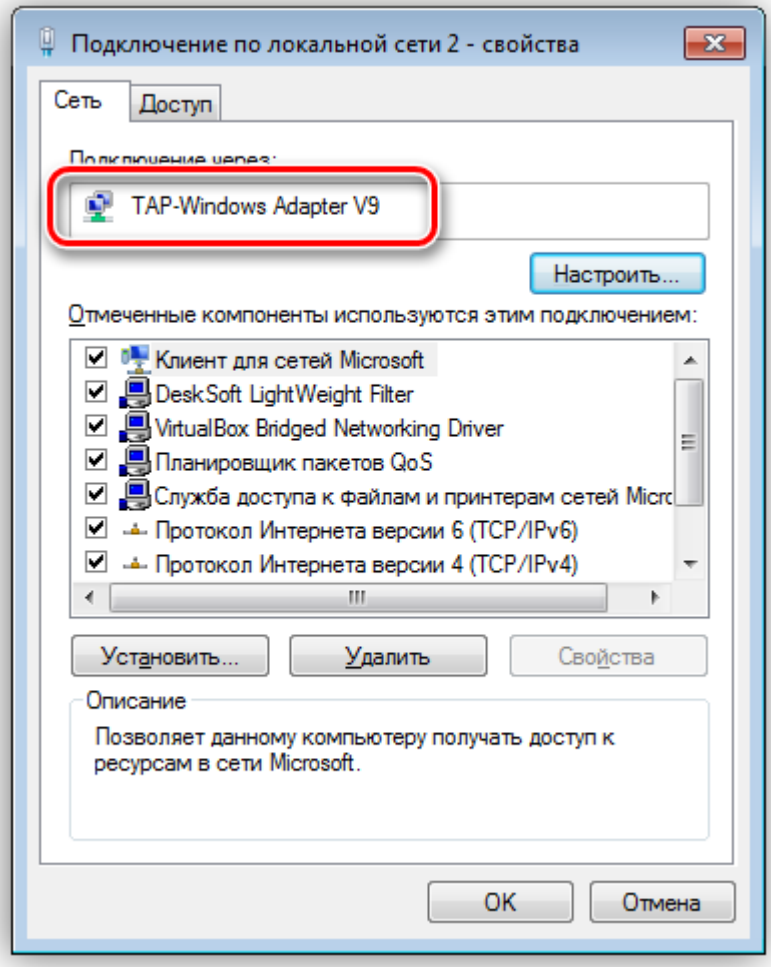

Рис 2.22

Переименовать его в “VPN Lumpics”. Это название совпадает с параметром “dev-node”в файле server.ovpn. Рис 2.23

Рис 2.23

Запустить службу нажатием сочетание клавиш Win+R, ведя в строку “services.msc” и нажать ENTER. Рис 2.24

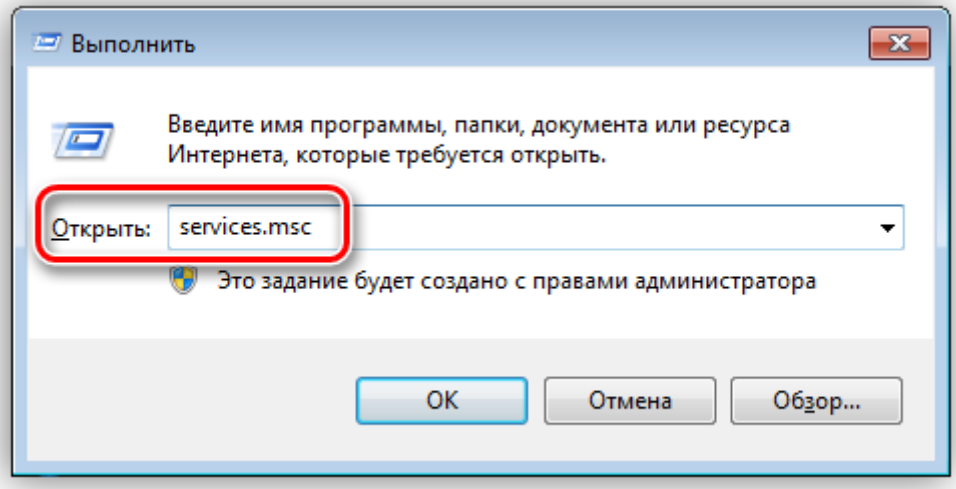

Рис 2.24

Найти сервис с названием “OpenVpnService”, кликнув правой кнопку мышки и открыть его свойства. Рис 2.25

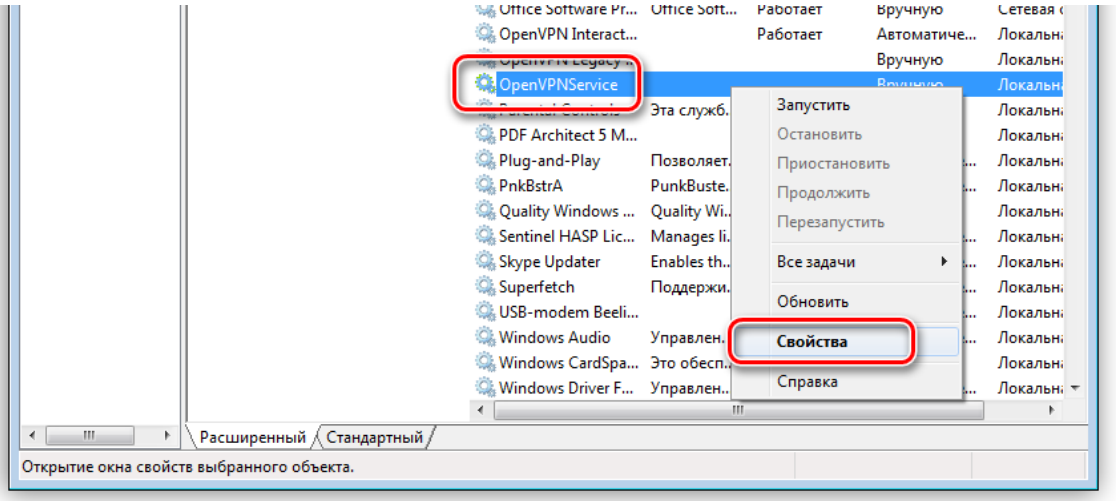

Рис 2.25

Тип запуска поменять на “Автоматически” запустить службу и нажать “Применить” Рис 2.26

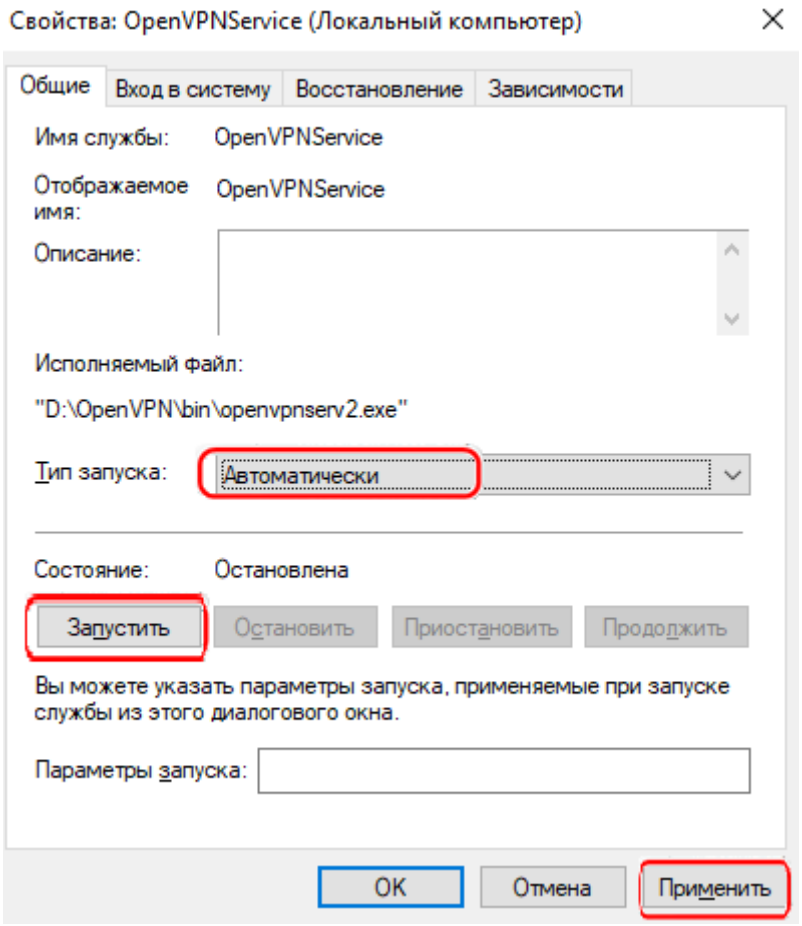

Рис 2.26

2.2Установка и настройка клиента OpenVPN

Для создания клиентских сертификатов и ключей нужно:

Открыть папку “easy-rsa”-“keys” и открываю файл “index.txt”. Рис 2.27 удалить все содержимое и сохранить.

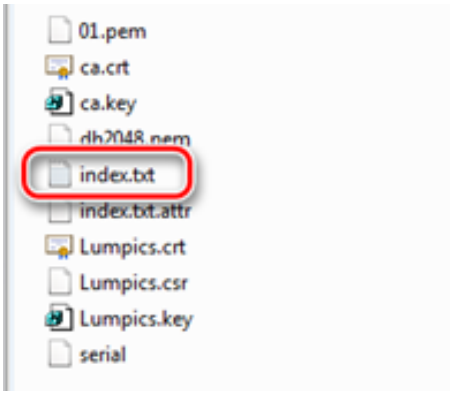

Рис 2.27

Открыть папку “easy-rsa” и запустить “Командную строку” (SHIFT+Правая кнопка мышки – Открыть окно команд).

Вести команду vars.bat, а затем создать клиентский сертификат с названием “vpn-client” командой “build-key.bat vpn-client” рис2.28

рис2.28

Это общий сертификат для всех машин в сети. Для повышения безопасности в дальнейшем можно сгенерировать для каждого компьютера свои файлы, но назвать их по-другому, например, “vpn-client1” и так далее. В этом случае необходимо будет повторять все действия, начиная с очистки index.txt.

Создать “config.ovpn” через Конфигуратор для этого нужно:

Открываем “Конфигуратор” и водим следующий поля:

IP Удалённого доступа.

Протокол.

ca ca.crt - файл сертификата для CA.

cert vpn-client.crt – файл сертификат клиента.

key vpn-client.key - файл ключ клиента.

dh dh2048.pem - файл dh.

и нажимаем на создать.

Для подключения клиента к серверу нужно:

Установить OpenVPN обычным способом на компьютер через какой будет производится подключения.

Перекинуть файлы vpn-client.crt, vpn-client.key, ca.crt, dh2048.pem и config.ovpn на компьютер и запускаю config.ovpn. После чего в трее значок поменяется на зеленый Рис 2.29

рис 2.29

2.2.1Тесты и Проверка Клиента соединения

Проверка скорости Интернета без подключения OpenVPN Рис 2.30

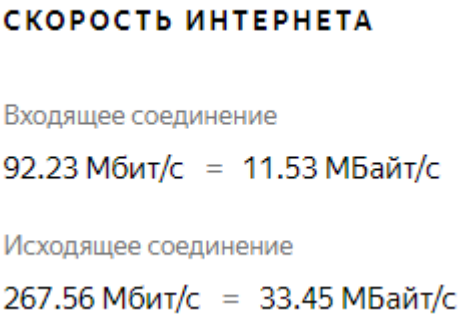

Рис 2.30

Проверка скорости Интернета с подключением OpenVPN Рис 2.31

Рис 2.31

Проверка подключения клиента к серверу организации

Прописываю локальный IP компьютера (через двойной обратный слеш ”\\”) организации на который есть доступ в локальной сети организации. Рис2.32

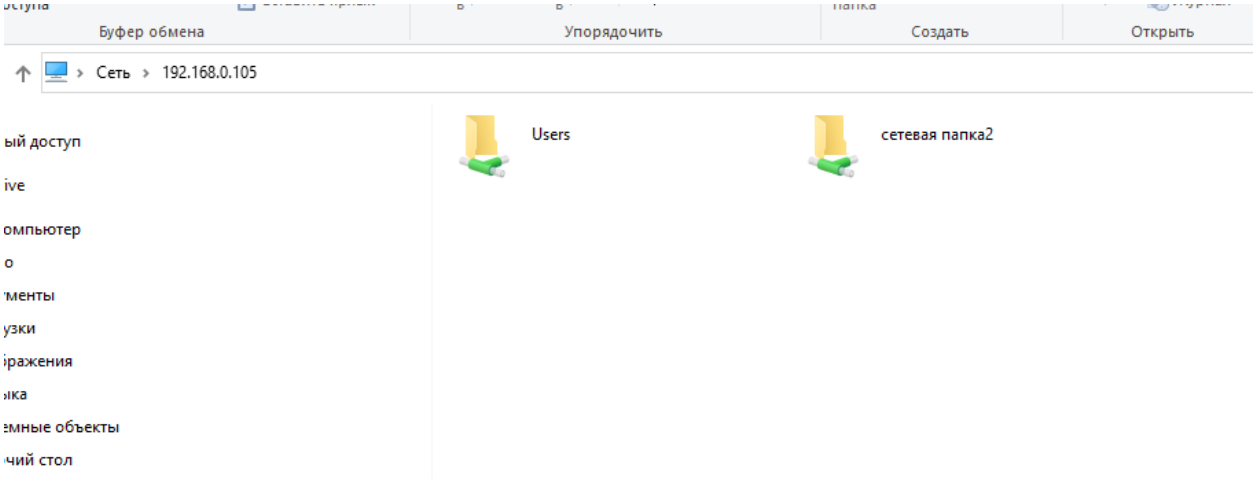

Рис 2.32

Проверка подключения серверу организации к клиенту

Прописываю локальный IP компьютера (через двойной обратный слеш ”\\”) сети клиента. Рис2.33

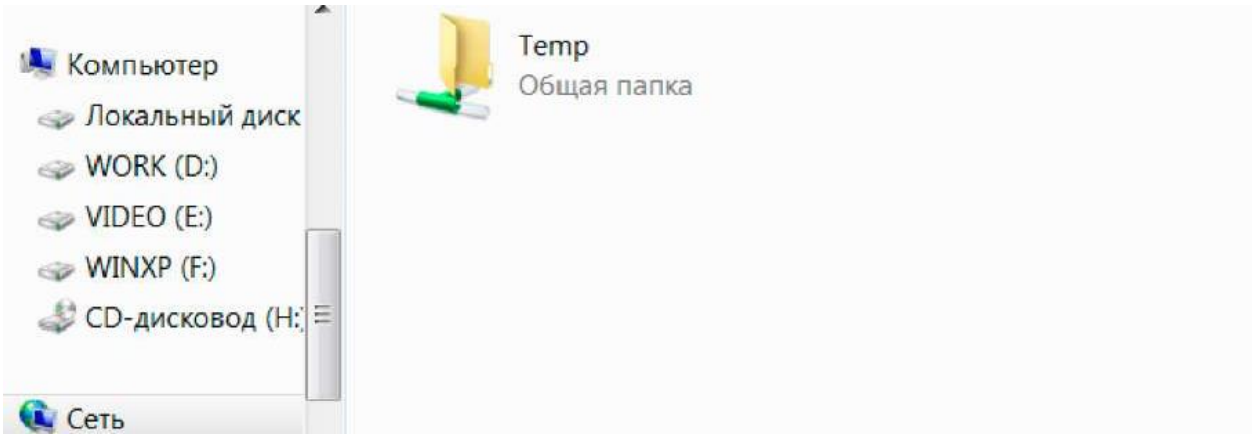

Рис2.33

Проверка сетевого окружения

Захожу в папку сеть с клиента рис 2.34

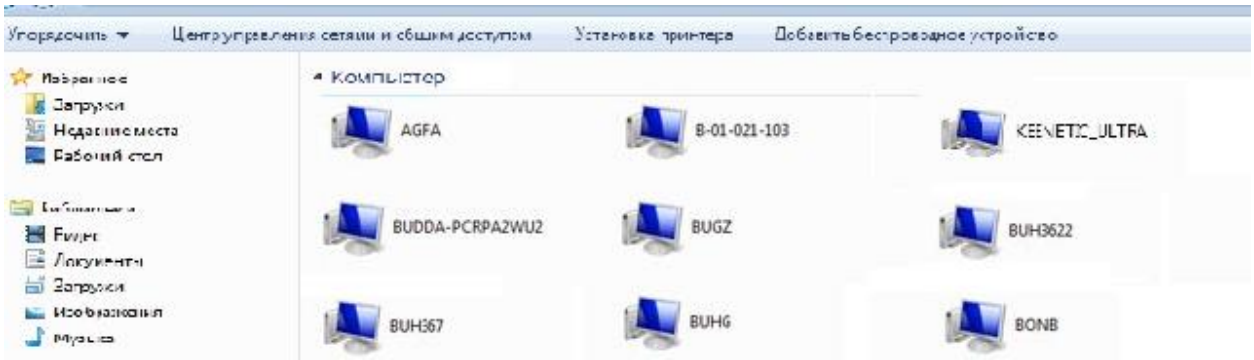

рис 2.34

Схема подключения клиента к серверу рис 2.35

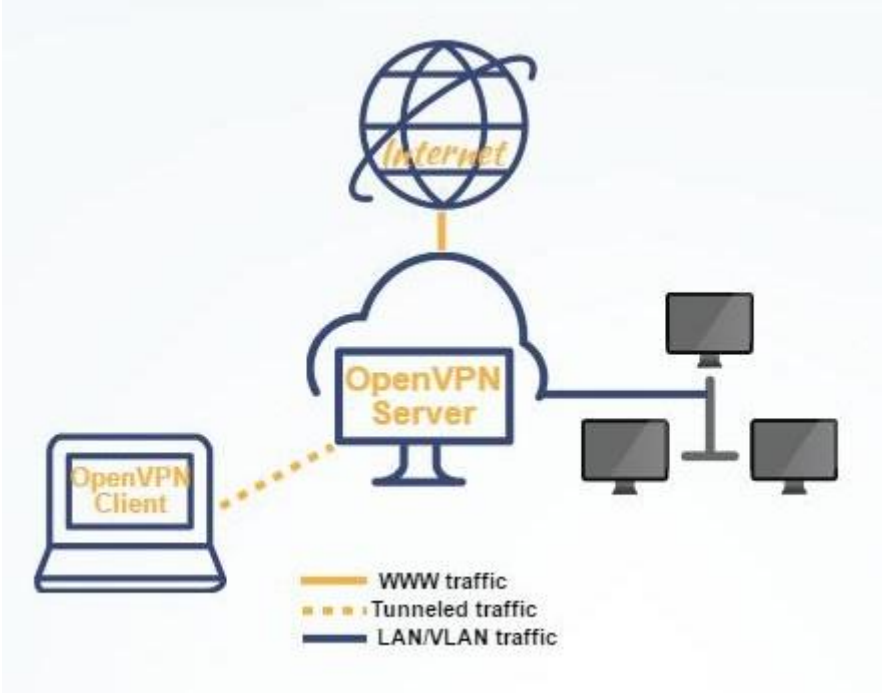

рис 2.35

Заключение

OpenVPN - свободная реализация технологии виртуальной частной сети (VPN) с открытым исходным кодом для создания зашифрованных каналов типа точка-точка или сервер-клиенты между компьютерами. Она позволяет устанавливать соединения между компьютерами, находящимися за NAT и сетевым экраном, без необходимости изменения их настроек

Теоретическая часть диплома описывает аспекты и термины, а также определение и состав: VPN, протоколы (TCP и UDP), протоколы шифрования и OpenVPN.

Практическая часть диплома описывает разработку OpenVPN для организации, основные идеи и концепции. Были создания удалённого доступа к локальной сети организации через Open VPN. Создания лёгкого конфигурации для клиента где не требуется для сотрудников организации никаких настройках на своем компьютере, а просто запуска файла конфигурации.

В данной дипломной работе были подробно рассмотрены и проанализирован: VPN, протоколы (TCP и UDP), протоколы шифрования и OpenVPN

Перед началом работы была поставлена цель дипломной работы:

- Разработать систему удалённого доступа к сети организации с помощью OpenVPN.

Для достижения этой цели были выполнены следующие задачи:

- Изучить теоретическую часть по виртуальным сетям, методов шифрования и протоколов передач данных
- Провести анализ виртуальных сетей, методов шифрования и протоколов передач данных
- Установить сервер и Настроить OpenVPN на предприятия
- Создать простой конфигуратор для клиентов

Список информационных источников

Книги одного автора

1. Баранова, Е.К. Информационная безопасность и защита информации[Текст]: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2017.

2. Баринов, В.В. Компьютерные сети: Учебник / В.В. Баринов, И.В. Баринов, А.В. Пролетарский. - М. [Текст]: Academia, 2018. - 192 с. Максимов, Н.В. Компьютерные сети: Учебное пособие / Н.В. Максимов, И.И. Попов. - М.: Форум, 2017.

3. Богданов-Катьков, Н.В. Интернет[Текст]: Новейший справочник / Н.В. Богданов-Катьков, А.А. Орлов. - М.: Эксмо, 2015

4. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам[Текст]: / Г.А. Бузов. - М.: ГЛТ, 2016.

5. Емельянова, Н.З. Защита информации в персональном компьютере[Текст]: Уч.пос / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. - М.: Форум, 2017.

6. Жданов, О. Н. Методика выбора ключевой информации для алгоритма блочного шифрования / О.Н. Жданов. - М. [Текст]: ИНФРА-М, 2015.

7. Камский, В. Защита личной информации в интернете, смартфоне и компьютере / В. Камский. - СПб. [Текст]: Наука и техника, 2017.

8. Крамаров, С.О. Криптографическая защита информации[Текст]: Учебное пособие / С.О. Крамаров, Е.Н. Тищенко, С.В. Соколов и др. - М.: Риор, 2019.

9. Литвинская, О. С. Основы теории передачи информации. Учебное пособие / О.С. Литвинская, Н.И. Чернышев. - М. [Текст]: КноРус, 2015

10.Малюк, А.А. Защита информации в информационном обществе[Текст]: Учебное пособие для вузов / А.А. Малюк. - М.: ГЛТ, 2015.

11.Мельников, В.П. Защита информации[Текст]: Учебник / В.П. Мельников. - М.: Академия, 2019.

12.Михайлов, Ю. Б. Научно-методические основы обеспечения безопасности защищаемых объектов / Ю.Б. Михайлов. - М. [Текст]: Горячая линия - Телеком, 2015

13.Олифер, В. Компьютерные сети. Принципы, технологии, протоколы[Текст]: Учебник / В. Олифер, Н. Олифер. - СПб.: Питер, 2016.

14.Таненбаум, Э. Компьютерные сети / Э. Таненбаум. - СПб. [Текст]: Питер, 2019.

15. Шувалов, В. П. Обеспечение показателей надежности телекоммуникационных систем и сетей / В.П. Шувалов. [Текст]:: Горячая линия - Телеком, 2015.

Книги двух авторов

16.Олифер В. Г., Олифер Н. П. Компьютерные сети. Принципы, технологии, протоколы[Текст]: Учебник для вузов. 5-е изд. — СПб: Питер, 2016.

Книги трех авторов

17.Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации [Текст] : учеб. пособие для студентов вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова – М. : Академия, 2014

Сайты в сети Интернет

18. Инструкция по настройке VPN-соединения для Windows 7. [ссылка]. [просмотрено 11.12.2019] http://www.tomtel.ru/tariffsandconnection/vpn/vpnconf7.html

19. Построение безопасных сетей на основе VPN. [ссылка]. [просмотрено 22.12.2019] http://www.aitishnik.ru/seti/postroenie-bezopasnich-setey-na-osnove-vpn.html

20. Применение OpenVPN для построения виртуальных частных сетей [ссылка]. [просмотрено 14.12.2019] https://lvee.org/ru/articles/149

21. Организация VPN-каналов между офисами при помощи OpenVPN[ссылка]. [просмотрено 10.01.2020] http://interface31.ru/tech_it/2011/09/organizaciya-vpn-kanalov-mezhdu-ofisami.html

22. Информационная технология. Криптографическая защита информации [ссылка]. [просмотрено 11.12.2019] www.tc26.ru/standard/gost/GOST_R_3412-2015

23. Лекция 8: Скоростные и беспроводные сети. [ссылка]. [просмотрено 11.12.2019] http://www.intuit.ru/studies/courses/57/57/lecture/1686?page=5

24. Руководство по настройке и установке OpenVPN [ссылка]. [просмотрено 03.01.2020] http://habrahabr.ru/post/233971/

25. Семь популярных VPN-сервисов. [ссылка]. [просмотрено 05.01.2019] http://www.computerra.ru/129276/sem-populyarnyih-vpn-servisov/

26. Виртуальные частные сети. [ссылка]. [просмотрено 11.12.2019] http://it-sektor.ru/virtual-nye-chastnye-seti.html

27. Туннельные протоколы VPN. [ссылка]. [просмотрено 06.12.2019] https://technet.microsoft.com/ru-ru/library/cc771298%28v=ws.10%29.aspx

28. Что такое VPN? [ссылка]. [просмотрено 13.12.2019] http://kb.netgear.ru/app/answers/detail/a_id/22363

29. Методы анонимности в сети. [ссылка]. [просмотрено 06.12.2019] http://habrahabr.ru/post/204266/

30. OpenVPN, краткое описание [ссылка]. [просмотрено 16.12.2019] https://7d3.ru/wiki/166

31. Алгоритм Диффи-Хелмана [ссылка]. [просмотрено 13.12.2019] http://dic.academic.ru/dic.nsf/ruwiki/212946

32. Список серверов openvpn [ссылка]. [просмотрено 16.12.2019] https://losst.ru/spisok-serverov-openvpn

33. PPTP [ссылка]. [просмотрено 10.12.2019] https://ru.wikipedia.org/wiki/PPTP

34. IPsec [ссылка]. [просмотрено 10.12.2019] https://ru.wikipedia.org/wiki/IPsec

35. Википедия – Open VPN. [ссылка]. [просмотрено 11.12.2019] https://ru.wikipedia.org/wiki/OpenVPN

36. Википедия - VPN. [ссылка]. [просмотрено 12.12.2019] https://ru.wikipedia.org/wiki/VPN

37. Виртуальные частные сети. [ссылка]. [просмотрено 12.12.2019] http://itsektor.ru/virtual-nye-chastnye-seti.html

38. История интернета: ARPANET [ссылка]. [просмотрено 12.12.2019] https://habr.com/ru/post/461177/

39. VPN. [ссылка]. [просмотрено 13.12.2019] http://www.cisco.com/web/RU/products/sw/netmgtsw/ps2327/index.html

40. Туннельные протоколы VPN. [ссылка]. [просмотрено 13.12.2019] https://technet.microsoft.com/ru-ru/library/cc771298%28=ws.10%29.apx

41. Что такое VPN? [ссылка]. [просмотрено 14.12.2019] https://technet.microsoft.com/ru-ru/library/cc731954%28v=ws.10%29.aspx

42. OpenVPN туннелирование сети [ссылка]. [просмотрено 14.12.2019] https://sourceforge.net/p/openvpn/mailman/message/13645972/

43. Создание VPN-подключения. [ссылка]. [просмотрено 06.01.2020] https://technet.microsoft.com/ru-ru/library/cc726062%28v=ws.10%29.aspx

44. Описание команд и параметров OpenVPN [ссылка]. [просмотрено 06.01.2016] https://vladimirmalikov.com/описание-команд-и-параметров-openvpn/

45. OpenVPN, о котором вы так мало знали [ссылка]. [просмотрено 09.12.2019] https://www.pvsm.ru/python/305082